In The Specification:

Please amend paragraph [0004], [0008], [0012], [0013] and [0015] as follows:

[0004] The operating method of a portable computer security system of the invention equips a portable computer with an EC, and the EC contains a security mechanism. In the operating method, a key is first provided. The key provides a signal sending to the EC to indicate whether the portable computer is to be locked. Next, if the EC detects that the portable computer is to be locked, the EC turns on the security mechanism. Then, the security mechanism determines whether the portable computer is hacked or is attempted to be hacked by a hacker; the security mechanism responds with a corresponding security action such as a security notice, an alarm, or a lock-up of the portable computer.

[0008] As a summary to the above description, the preferred embodiment of the present invention utilizes an external device, an internal device unit, or an internal function of the portable computer to be a security key. Then, via a signal produced by a security key related circuit, the EC learns whether the portable computer is to be locked. Upon the EC recognizing that the portable computer is to be locked, the EC turns on the security mechanism. Further, the security mechanism gives out an alarm, a warning message, or a security action when a hacking action is detected. Therefore, the preferred embodiment of the present invention equips a portable computer with a security mechanism to secure data in the portable computer.

[0012] Referring to Fig. 1, a portable computer 10 of the preferred embodiment of the present invention is depicted. The portable computer 10 comprises an EC 102, a computer system 104, an other-related system 106, power unit 108, and a key 110. The

EC 102 is used to control an operation of the computer system 104 and the other-related system 106, and is equipped with a security mechanism. The key 110 accompanying with a key circuit provides a signal to the EC 102 to indicate whether the portable computer 10 is to be locked. The key 110 is, for instance, an internal key unit or an internal key function of the portable computer 10. For example, the key 110 can be a special key on a keyboard; when the key is pressed down, the EC 102 learns that the portable computer 10 is to be locked. Or, the key 110 can be an unit or a function of an external device. For instance, the key 110 can be a button on a infrared remote control device; when the button is pressed down, an infrared signal is transmitted to the portable computer 10, and the EC activates the security mechanism accordingly. It is clear to those skilled in the art that the key 110 is any kind of apparatus that allows the EC 102 to learn whether the portable computer 10 is to be locked.

[0013] Referring to Fig. 2, a flow-chart diagram of the operating method of the portable computer security mechanism of the preferred embodiment of the present invention is depicted. In the operating method, fist a function of the key 110 is assigned to an external device, or an internal device or function of the portable computer 10. Then, via the key 110 related circuit in the portable computer 10, a signal is generated to inform the EC 102 whether the portable computer is to be locked as demonstrated in step S202. If the EC 102 learns that the portable computer is not to be locked, the EC 102 allows the portable computer to function normally as demonstrated in step S204. On the other hand, if the EC 102 learns that the portable computer is to be locked, the EC 102 turns on the security mechanism accordingly as demonstrated in step S206. The security mechanism provides security functions including preventing the portable computer 10 to turn on from

a hacker, preventing a keyboard input from a hacker, preventing a mouse input from a hacker, and providing a security signal to BIOS to secure a BIOS data from being changed. Next, the EC 102 determines whether the portable computer 10 is hacked or is being hacked by a hacker as demonstrated in step S208. The EC 102 goes back to step S202, if the portable computer 10 is not hacked or is not being hacked by a hacker. However, if the EC 102 determines that the portable computer 10 is hacked or is being hacked, the EC 102 turns on a security function as demonstrated in step S210. Further, a follow-up security procedure is taken place as demonstrated in step S212. The follow-up security procedure includes turning off the portable computer, shutting down a monitor of the portable computer, or executing a specific security program. Taking one step further, a related security action includes an attack or a self-destroy action.

[0015] As a summary to the above description, the preferred embodiment of the present invention utilizes an external device, or an internal device or an internal function of the portable computer 10 to be a security key. Then, via a signal produced by a security key related circuit, the EC 102 learns whether the portable computer 10 is to be locked. Upon the EC 102 recognizing that the portable computer 10 is to be locked, the EC 102 turns on the security mechanism. Further, the security mechanism gives out an alarm, a warning message, or a security action when a hacking action is detected. Therefore, the preferred embodiment of the present invention equips a portable computer with a security mechanism to secure data in the portable computer 10.